

WHAT IS CLAIMED IS:

1. In an encryption-decryption apparatus for encryption of data and decryption of encrypted data, the encryption-decryption apparatus comprising a variable configuration circuit arrangement as an encryption-decryption circuit,

5 wherein an encryption-decryption operation is performed by using circuit data of the variable configuration circuit arrangement as a secret key.

2. An encryption-decryption apparatus according to claim 1, further comprising a plurality of circuit data of the variable configuration circuit arrangement,

5 wherein an encryption-decryption operation is performed according to different types of algorithms by feeding after selecting the circuit data of the variable configuration circuit arrangement from circuit data selection information for encryption-decryption.

3. An encryption-decryption apparatus comprising:
a transmitting apparatus to encrypt input data to output encrypted data;

5 a network to transmit the encrypted data; and
a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

10 wherein the transmitting apparatus includes a variable configuration processing circuit for encryption, and a ROM to output circuit data serving as a secret key to the variable configuration processing circuit, and the receiving apparatus including a variable configuration processing circuit for decryption, and a ROM to output circuit data serving as a secret key to the variable configuration

0935172-04501

processing circuit.

4. The encryption-decryption apparatus according to claim 3, wherein the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to output as held data the input data which has been held therein;

5 a flash ROM in which data of a cryptographic algorithm is stored; and

a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in 10 the flash ROM by the first circuit data, take as input second circuit data from the flash ROM when the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data,

15 and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been 20 held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, 25 update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal

PCT/US2017/048660

circuit is updated, and send output data obtained by decryption of the

30 held data.2

5. The encryption-decryption apparatus according to claim 3,
wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data,
and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input
data until a circuit is completely updated, and receive a completion
posting signal to output as held data the input data which has been
held therein; and

10 a variable configuration processing circuit to update the circuit
for encryption by using the circuit data, output the completion posting
signal to the encryption/decryption data holding portion when the
circuit is completely updated, and send output data obtained by
encryption through an updated circuit configuration, and

15 the receiving apparatus having:

a circuit data extracting portion to take as input the encrypted
output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output
data until the circuit is completely updated, and receive a completion
posting signal to output as held data the encrypted output data which
20 has been held therein; and

25 a variable configuration processing circuit to update a circuit for
decryption by using the circuit data, output the completion posting
signal to the encryption/decryption data holding portion after the
circuit is completely updated, and send output data obtained by
decryption through an updated circuit configuration.

6. The encryption-decryption apparatus according to claim 3,

2025 RELEASE UNDER E.O. 14176

wherein the variable configuration processing circuit is a Field Programmable Gate Array.

7. An encryption-decryption apparatus according to claim 3, wherein the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to output as held data the input data which has been held therein;

5 a flash ROM in which data of a cryptographic algorithm is stored; and

10 a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM when the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data;

15 the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been held therein;

20 a flash ROM in which data of a cryptographic algorithm is stored;

a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input 25 second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal

0985172 041307

circuit is updated, and send output data obtained by decryption of the held data; and

30 the variable configuration processing circuit is a Field Programmable Gate Array.

8. The encryption-decryption apparatus according to claim 3, wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data, and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input data until a circuit is completely updated, and receive a completion posting signal to output as held data the input data which has been held therein; and

10 a variable configuration processing circuit to update the circuit for encryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion when the circuit is completely updated, and send output data obtained by encryption through an updated circuit configuration, and

the receiving apparatus having:

15 a circuit data extracting portion to take as input the encrypted output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output data until the circuit is completely updated, and receive a completion posting signal to output as held data the encrypted output data which has been held therein;

20 a variable configuration processing circuit to update a circuit for decryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion after the circuit is completely updated, and send output data obtained by decryption through an updated circuit configuration; and

TOSYHD-24792860

the variable configuration processing circuit is a Field Programmable Gate Array.

9. An encryption-decryption apparatus comprising:
 - a transmitting apparatus to encrypt input data to output encrypted data;
 - a network to transmit the encrypted data; and
- 5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,
 - wherein the transmitting apparatus having:
 - 10 a data analyzing portion to analyze information of the input data according to a predetermined instruction, and output updating information after decoding;
 - a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;
 - 15 a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM to send circuit data for encryption;
 - 20 a variable configuration processing circuit to update an own internal circuit depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM, output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data; and
 - 25 an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the input data which has been held therein to the variable configuration processing circuit for encryption, and
 - the receiving apparatus having:

10370-22736800

a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network,
30 and output updating information after decoding;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM
35 to send circuit data for decryption;

a variable configuration processing circuit to update an own internal circuit for decryption depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM, output a completion posting signal when the update of the internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of the held input data; and
40

an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the encrypted data which has been held therein to the variable configuration processing circuit for decryption.
45

10. The encryption-decryption apparatus according to claim 9, wherein the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to
5 output as held data the input data which has been held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

10 a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM when the update is completed to update an

09535472.101440

own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data,

15 and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been
20 held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by decryption of the held data.

11. The encryption-decryption apparatus according to claim 9, wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data, and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input data until a circuit is completely updated, and receive a completion posting signal to output as held data the input data which has been held therein; and

a variable configuration processing circuit to update the circuit

10 for encryption by using the circuit data, output the completion posting

TOP SECRET//COMINT

signal to the encryption/decryption data holding portion when the circuit is completely updated, and send output data obtained by encryption through an updated circuit configuration, and

the receiving apparatus having:

- 15 a circuit data extracting portion to take as input the encrypted output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output data until the circuit is completely updated, and receive a completion posting signal to output as held data the encrypted output data which
20 has been held therein; and

a variable configuration processing circuit to update a circuit for decryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion after the circuit is completely updated, and send output data obtained by decryption through an updated circuit configuration.

12. The encryption-decryption apparatus according to claim 9, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

13. The encryption-decryption apparatus according to claim 9, wherein the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to
5 output as held data the input data which has been held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in
10 the flash ROM by the first circuit data, take as input second circuit

CONFIDENTIAL

data from the flash ROM when the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data,

15 and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been
20 held therein;

a flash ROM in which data of a cryptographic algorithm is stored;

25 a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by decryption of the
30 held data; and

the variable configuration processing circuit is a Field Programmable Gate Array.

14. The encryption-decryption apparatus according to claim 9, wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data, and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input data until a circuit is completely updated, and receive a completion posting signal to output as held data the input data which has been

TOSR#0-22755600

held therein; and

10 a variable configuration processing circuit to update the circuit for encryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion when the circuit is completely updated, and send output data obtained by encryption through an updated circuit configuration, and

the receiving apparatus having:

15 a circuit data extracting portion to take as input the encrypted output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output data until the circuit is completely updated, and receive a completion posting signal to output as held data the encrypted output data which has been held therein;

20 a variable configuration processing circuit to update a circuit for decryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion after the circuit is completely updated, and send output data obtained by decryption through an updated circuit configuration; and

25 the variable configuration processing circuit is a Field Programmable Gate Array.

15. An encryption-decryption apparatus comprising:

a transmitting apparatus to encrypt input data to output encrypted data;

a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

wherein the transmitting apparatus having:

a data analyzing portion to analyze information of the input data

1084012279360

10 according to a predetermined instruction, and output analysis information;

a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;

15 a Field Programmable Gate Array (FPGA) circuit data generating portion to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a circuit configuration, and generate and output second circuit data;

20 a selector to select the plurality of circuit data according to an instruction of the selection signal, and output the first circuit data for encryption to the FPGA circuit data generating portion depending upon the selected circuit data;

25 a variable configuration processing circuit to update an own internal circuit depending upon the second circuit data output from the FPGA circuit data generating portion, output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data;

30 an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input data the input data which has been held therein to the variable configuration processing circuit, and

the receiving apparatus having:

35 a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network, and output analysis data;

a plurality of FPGA circuit data generating portions to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a

T08740-2273850

- 9885172-041804
- 40 circuit configuration, and generate and output second circuit data;
a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;
a selector to select the plurality of circuit data according to an instruction in the selection signal, and output to the FPGA circuit data generating portion the first circuit data used for decryption depending upon the selected circuit data;
a variable configuration processing circuit to update an own internal circuit for decryption depending upon the second circuit data output from the FPGA circuit data generating portion, output a completion posting signal when the update of the internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of held input data; and
an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input data the input data which has been held therein to the variable configuration processing circuit.
- 50
- 55

16. The encryption-decryption apparatus according to claim 15, wherein the transmitting apparatus having:

- 5 an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to output as held data the input data which has been held therein;
- a flash ROM in which data of a cryptographic algorithm is stored; and
- 10 a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM when the update is completed to update an own internal circuit, output the completion posting signal to the

15 encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data,

15 and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been
20 held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

25 a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by decryption of the
30 held data.

17. The encryption-decryption apparatus according to claim 15, wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data, and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input data until a circuit is completely updated, and receive a completion posting signal to output as held data the input data which has been held therein; and

10 a variable configuration processing circuit to update the circuit for encryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion when the

TESTIMONY OF JAMES G. BROWN

circuit is completely updated, and send output data obtained by encryption through an updated circuit configuration, and

the receiving apparatus having:

15 a circuit data extracting portion to take as input the encrypted output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output data until the circuit is completely updated, and receive a completion posting signal to output as held data the encrypted output data which
20 has been held therein; and

a variable configuration processing circuit to update a circuit for decryption by using the circuit data, output the completion posting signal to the encryption/decryption data holding portion after the circuit is completely updated, and send output data obtained by decryption through an updated circuit configuration.

18. The encryption-decryption apparatus according to claim 15, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

19. An encryption-decryption apparatus according to claim 15, wherein the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and receive the completion posting signal to
5 output as held data the input data which has been held therein;

a flash ROM in which data of a cryptographic algorithm is stored; and

10 a variable configuration processing circuit to take as input the input data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM when the update is completed to update an

1020140-2735890

own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by encryption of the held data,

15 and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and receive the completion posting signal to output as held data the output data which has been
20 held therein;

a flash ROM in which data of a cryptographic algorithm is stored;

a variable configuration processing circuit to take as input the encrypted output data, output first circuit data to the flash ROM, update data in the flash ROM by the first circuit data, take as input second circuit data from the flash ROM after the update is completed to update an own internal circuit, output the completion posting signal to the encryption/decryption data holding portion after the internal circuit is updated, and send output data obtained by decryption of the held data; and
25
30

the variable configuration processing circuit is a Field Programmable Gate Array.

20. The encryption-decryption apparatus according to claim 15, wherein the transmitting apparatus having:

a circuit data extracting portion to take as input the input data, and generate and output circuit data;

5 an encryption/decryption data holding portion to hold the input data until a circuit is completely updated, and receive a completion posting signal to output as held data the input data which has been held therein; and

00859572 00740314

a variable configuration processing circuit to update the circuit
10 for encryption by using the circuit data, output the completion posting
signal to the encryption/decryption data holding portion when the
circuit is completely updated, and send output data obtained by
encryption through an updated circuit configuration, and

the receiving apparatus having:

15 a circuit data extracting portion to take as input the encrypted
output data, and generate and output circuit data;

an encryption/decryption data holding portion to hold the output
data until the circuit is completely updated, and receive a completion
posting signal to output as held data the encrypted output data which
20 has been held therein;

25 a variable configuration processing circuit to update a circuit for
decryption by using the circuit data, output the completion posting
signal to the encryption/decryption data holding portion after the
circuit is completely updated, and send output data obtained by
decryption through an updated circuit configuration; and

the variable configuration processing circuit is a Field
Programmable Gate Array.

21. An encryption-decryption apparatus comprising:

a transmitting apparatus to encrypt input data to output
encrypted data;

a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data
transmitted through the network, perform a decryption operation, and
send output data obtained by the decryption,

10 wherein the transmitting apparatus includes a variable
configuration processing circuit for encryption, and a ROM to output
circuit data serving as a secret key to the variable configuration

TO87462798860

processing circuit, and the receiving apparatus including a variable configuration processing circuit for decryption, and a ROM to output circuit data serving as a secret key to the variable configuration processing circuit;

- 15 the transmitting apparatus having:
 an encryption/decryption data holding portion to take as input
and hold the input data, and take as input a circuit update posting
signal to output as held data the input data which has been held
therein;

20 a random generator to generate an encryption code;
 a data analyzing portion to make a decision as to whether the
input data is data to be encrypted or data to be decrypted, and output
analysis data used to instruct to enable data from the random
generator in the case of data to be encrypted or instruct to enable a
25 secret key in the case of data to be decrypted;
 an FPGA circuit data generating portion to generate and output
first circuit data according to the posted analysis data;
 a plurality of ROMs in which data used for specification of a
cryptographic algorithm is stored;

30 a selector to take circuit data from the plurality of ROMs
depending upon the first circuit data, and output second circuit data
used for specification of a cryptographic algorithm; and
 a variable configuration processing circuit to take as input the
second circuit data to output the circuit update posting signal so as to
35 stop output of the held data from the encryption/decryption data
holding portion, update an own internal circuit for encryption by the
second circuit data, stop the circuit update posting signal when the
update is completed, and resume output of the held data to output the
encrypted output data, and

40 the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and take as input a circuit update posting signal to output as held data the output data which has been held therein;

- 45 a random generator to generate an encryption code;
a data analyzing portion to make a decision as to whether the encrypted output data is data to be encrypted or data to be decrypted, and output analysis data to instruct to enable data from the random generator in the case of data to be encrypted or instruct to enable a
50 secret key in the case of data to be decrypted;
an FPGA circuit data generating portion to generate and output first circuit data according to the posted analysis data;
a plurality of ROMs in which data used for specification of a cryptographic algorithm is stored;
55 a selector to take circuit data from the plurality of ROMs depending upon the first circuit data, and output second circuit data used for specification of a cryptographic algorithm; and
a variable configuration processing circuit to take as input the second circuit data to output the circuit update posting signal so as to
60 stop output of the held data from the encryption/decryption data holding portion, update an own internal circuit for decryption by the second circuit data, stop the circuit update posting signal when the update is completed, and resume output of the held data to output the decrypted output data.

22. The encryption-decryption apparatus according to claim 21, wherein the plurality of ROMs data are data from a plurality of data circuits implemented via hardware, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion,
5 and the FPGA circuit data generating portion outputting second

201401271428360

circuit data to the variable configuration processing circuit.

23. The encryption-decryption apparatus according to claim 21, wherein the plurality of ROMs data are data from a plurality of data circuit portions implemented via hardware, the random generator being a timer to generate and output a selector control signal at 5 regular intervals, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion, and the FPGA circuit data generating portion outputting second circuit data to the variable configuration processing circuit.

24. The encryption-decryption apparatus according to claim 21, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

25. An encryption-decryption apparatus comprising:
a transmitting apparatus to encrypt input data to output encrypted data;

a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

wherein the transmitting apparatus having:

10 a data analyzing portion to analyze information of the input data according to a predetermined instruction, and output updating information after decoding;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

15 a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM

09835172.041301

to send circuit data for encryption;

a variable configuration processing circuit to update an own internal circuit depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM,
20 output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data; and

an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the input
25 data which has been held therein to the variable configuration processing circuit for encryption;

the receiving apparatus having:

a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network,
30 and output updating information after decoding;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM
35 to send circuit data for decryption;

a variable configuration processing circuit to update an own internal circuit for decryption depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM, output a completion posting signal when the update of the
40 internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of the held input data; and

an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the encrypted data which has been held therein to the variable configuration processing circuit for decryption
45

009885472041801

the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and take as input a circuit update posting signal to output as held data the input data which has been held therein;

50 a random generator to generate an encryption code;

a data analyzing portion to make a decision as to whether the input data is data to be encrypted or data to be decrypted, and output analysis data used to instruct to enable data from the random generator in the case of data to be encrypted or instruct to enable a secret key in the case of data to be decrypted;

55 an FPGA circuit data generating portion to generate and output first circuit data according to the posted analysis data;

60 a plurality of ROMs in which data used for specification of a cryptographic algorithm is stored;

a selector to take circuit data from the plurality of ROMs depending upon the first circuit data, and output second circuit data used for specification of a cryptographic algorithm; and

65 a variable configuration processing circuit to take as input the second circuit data to output the circuit update posting signal so as to stop output of the held data from the encryption/decryption data holding portion, update an own internal circuit for encryption by the second circuit data, stop the circuit update posting signal when the update is completed, and resume output of the held data to output the encrypted output data, and

70 the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and take as input a circuit update posting signal to output as held data the output data which has been held therein;

TOP SECRET//SI//FOUO

a random generator to generate an encryption code;

80 a data analyzing portion to make a decision as to whether the encrypted output data is data to be encrypted or data to be decrypted, and output analysis data to instruct to enable data from the random generator in the case of data to be encrypted or instruct to enable a secret key in the case of data to be decrypted;

an FPGA circuit data generating portion to generate and output first circuit data according to the posted analysis data;

85 a plurality of ROMs in which data used for specification of a cryptographic algorithm is stored;

a selector to take circuit data from the plurality of ROMs depending upon the first circuit data, and output second circuit data used for specification of a cryptographic algorithm; and

90 a variable configuration processing circuit to take as input the second circuit data to output the circuit update posting signal so as to stop output of the held data from the encryption/decryption data holding portion, update an own internal circuit for decryption by the second circuit data, stop the circuit update posting signal when the update is completed, and resume output of the held data to output the 95 decrypted output data.

26. The encryption-decryption apparatus according to claim 25, wherein the plurality of ROMs data are data from a plurality of data circuits implemented via hardware, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion, 5 and the FPGA circuit data generating portion outputting second circuit data to the variable configuration processing circuit.

27. An encryption-decryption apparatus according to claim 25, wherein the plurality of ROMs data are data from a plurality of data

4084107-27T938860

circuit portions implemented via hardware, the random generator being a timer to generate and output a selector control signal at regular intervals, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion, and the FPGA circuit data generating portion outputting second circuit data to the variable configuration processing circuit.

28. The encryption-decryption apparatus according to claim 25, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

29. An encryption-decryption apparatus comprising:

a transmitting apparatus to encrypt input data to output encrypted data;

a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

the transmitting apparatus having:

10 a data analyzing portion to analyze information of the input data according to a predetermined instruction, and output analysis information;

a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;

15 a Field Programmable Gate Array (hereinafter abbreviated to as FPGA) circuit data generating portion to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a circuit configuration, and generate and output second circuit data;

a selector to select the plurality of circuit data according to an

103700-24750860

20 instruction of the selection signal, and output the first circuit data for encryption to the FPGA circuit data generating portion depending upon the selected circuit data;

25 a variable configuration processing circuit to update an own internal circuit depending upon the second circuit data output from the FPGA circuit data generating portion, output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data; and

30 an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input data the input data which has been held therein to the variable configuration processing circuit;

the receiving apparatus having:

35 a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network, and output analysis data;

40 a plurality of FPGA circuit data generating portions to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a circuit configuration, and generate and output second circuit data;

a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;

45 a selector to select the plurality of circuit data according to an instruction in the selection signal, and output to the FPGA circuit data generating portion the first circuit data used for decryption depending upon the selected circuit data;

a variable configuration processing circuit to update an own internal circuit for decryption depending upon the second circuit data output from the FPGA circuit data generating portion, output a

YOSHIO-279880

50 completion posting signal when the update of the internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of held input data; and

an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input
55 data the input data which has been held therein to the variable configuration processing circuit;

the transmitting apparatus further comprising:

an encryption/decryption data holding portion to take as input and hold the input data, and take as input a circuit update posting signal to output as held data the input data which has been held therein;
60

a random generator to generate an encryption code;

a data analyzing portion to make a decision as to whether the input data is data to be encrypted or data to be decrypted, and output analysis data used to instruct to enable data from the random generator in the case of data to be encrypted or instruct to enable a secret key in the case of data to be decrypted;
65

an FPGA circuit data generating portion to generate and output first circuit data according to the posted analysis data;

70 a plurality of ROMs in which data used for specification of a cryptographic algorithm is stored;

a selector to take circuit data from the plurality of ROMs depending upon the first circuit data, and output second circuit data used for specification of a cryptographic algorithm; and

75 a variable configuration processing circuit to take as input the second circuit data to output the circuit update posting signal so as to stop output of the held data from the encryption/decryption data holding portion, update an own internal circuit for encryption by the second circuit data, stop the circuit update posting signal when the

108747-2/TSC860

80 update is completed, and resume output of the held data to output the encrypted output data, and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and take as input a circuit update

85 posting signal to output as held data the output data which has been held therein;

a random generator to generate an encryption code;

a data analyzing portion to make a decision as to whether the encrypted output data is data to be encrypted or data to be decrypted,

90 and output analysis data to instruct to enable data from the random generator in the case of data to be encrypted or instruct to enable a secret key in the case of data to be decrypted;

an FPGA circuit data generating portion to generate and output first circuit data according to the posted analysis data;

95 a plurality of ROMs in which data used for specification of a cryptographic algorithm is stored;

a selector to take circuit data from the plurality of ROMs depending upon the first circuit data, and output second circuit data used for specification of a cryptographic algorithm; and

100 a variable configuration processing circuit to take as input the second circuit data to output the circuit update posting signal so as to stop output of the held data from the encryption/decryption data holding portion, update an own internal circuit for decryption by the second circuit data, stop the circuit update posting signal when the 105 update is completed, and resume output of the held data to output the decrypted output data.

30. An encryption-decryption apparatus according to claim 29, wherein the plurality of ROMs data are data from a plurality of data

T081404-2742660

circuits implemented via hardware, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion, 5 and the FPGA circuit data generating portion outputting second circuit data to the variable configuration processing circuit.

31. The encryption-decryption apparatus according to claim 29, wherein the plurality of ROMs data are data from a plurality of data circuit portions implemented via hardware, the random generator being a timer to generate and output a selector control signal at 5 regular intervals, the selector outputting circuit data as first circuit data to the FPGA circuit data generating portion, and the FPGA circuit data generating portion outputting second circuit data to the variable configuration processing circuit.

32. An encryption-decryption apparatus according to claim 29, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

33. An encryption-decryption apparatus comprising:
a transmitting apparatus to encrypt input data to output encrypted data;
5 a network to transmit the encrypted data; and
a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,
wherein the transmitting apparatus includes a variable configuration processing circuit for encryption, and a read-only memory (ROM) to output circuit data serving as a secret key to the variable configuration processing circuit, and the receiving apparatus including a variable configuration processing circuit for decryption,

003142-2745968860

and a read-only memory (ROM) to output circuit data serving as a secret key to the variable configuration processing circuit;

15 the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and take as input a circuit update posting signal to output as held data the input data which has been held therein;

20 a timer to generate and output a selector control signal at regular intervals;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

25 a selector to select the plurality of ROMs depending upon the selector control signal to take circuit data for encryption, and output circuit data used for specification of a cryptographic algorithm; and

30 a variable configuration processing circuit to receive the circuit data to output the circuit update posting signal, stop output of the held data, update an own internal circuit configuration depending upon the circuit data, stop the circuit update posting signal when the update is completed so as to resume output of the held data from the encryption/decryption data holding portion, and take as input the held data to perform an encryption operation through an updated internal circuit configuration so as to send encrypted output data, and

35 the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and take as input a circuit update posting signal so as to output as held data the input data which has been held therein;

40 a timer to generate and output a selector control signal at regular intervals;

a plurality of ROMs in which circuit data used for specification of

09836172-003404

a cryptographic algorithm is stored;

45 a selector to select the plurality of ROMs depending upon the selector control signal to take circuit data for encryption, and output circuit data used for specification of a cryptographic algorithm; and

50 a variable configuration processing circuit to output the circuit update posting signal in response to the circuit data so as to stop output of the held data, update an own internal circuit configuration depending upon the circuit data, stop the circuit update posting signal when the update is completed so as to resume output of the held data from the encryption/decryption data holding portion, and take as input the held data to perform a decryption operation through an updated internal circuit configuration so as to send decrypted output data.

34. The encryption-decryption apparatus according to claim 33, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

35. An encryption-decryption apparatus comprising:

a transmitting apparatus to encrypt input data to output encrypted data;

a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

wherein the transmitting apparatus having:

10 a data analyzing portion to analyze information of the input data according to a predetermined instruction, and output updating information after decoding;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

TOSTKOD-EY758653

a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM to send circuit data for encryption;

a variable configuration processing circuit to update an own internal circuit depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM,

20 output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data; and

an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the input data which has been held therein to the variable configuration processing circuit for encryption, and

the receiving apparatus having:

a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network, and output updating information after decoding;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

a selector to select the plurality of ROMs according to an instruction in the updating information, and cause the selected ROM 35 to send circuit data for decryption;

a variable configuration processing circuit to update an own internal circuit for decryption depending upon the circuit data used for specification of the cryptographic algorithm according to selection of the ROM, output a completion posting signal when the update of the 40 internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of the held input data; and

an encryption/decryption data holding portion to receive the completion posting signal, and output as the held input data the

45 encrypted data which has been held therein to the variable configuration processing circuit for decryption.

the transmitting apparatus having:

an encryption/decryption data holding portion to take as input and hold the input data, and take as input a circuit update posting signal to output as held data the input data which has been held 50 therein;

a timer to generate and output a selector control signal at regular intervals;

a plurality of ROMs in which circuit data used for specification of 55 a cryptographic algorithm is stored;

55 a selector to select the plurality of ROMs depending upon the selector control signal to take circuit data for encryption, and output circuit data used for specification of a cryptographic algorithm; and

60 a variable configuration processing circuit to receive the circuit data to output the circuit update posting signal, stop output of the held data, update an own internal circuit configuration depending upon the circuit data, stop the circuit update posting signal when the update is completed so as to resume output of the held data from the encryption/decryption data holding portion, and take as input the held data to perform an encryption operation through an updated internal 65 circuit configuration so as to send encrypted output data, and

the receiving apparatus having:

an encryption/decryption data holding portion to take as input and hold the encrypted output data, and take as input a circuit update 70 posting signal so as to output as held data the input data which has been held therein;

a timer to generate and output a selector control signal at regular intervals;

a plurality of ROMs in which circuit data used for specification of

TOP SECRET//SI//REL TO USA, FVEY, UK, CAN, AUS

a cryptographic algorithm is stored;

75 a selector to select the plurality of ROMs depending upon the selector control signal to take circuit data for encryption, and output circuit data used for specification of a cryptographic algorithm; and

80 a variable configuration processing circuit to output the circuit update posting signal in response to the circuit data so as to stop output of the held data, update an own internal circuit configuration depending upon the circuit data, stop the circuit update posting signal when the update is completed so as to resume output of the held data from the encryption/decryption data holding portion, and take as input the held data to perform a decryption operation through an updated internal circuit configuration so as to send decrypted output data.

85 36. The encryption-decryption apparatus according to claim 35, wherein the variable configuration processing circuit is a Field Programmable Gate Array.

37. An encryption-decryption apparatus comprising:

 a transmitting apparatus to encrypt input data to output encrypted data;

 a network to transmit the encrypted data; and

5 a receiving apparatus to take as input the encrypted data transmitted through the network, perform a decryption operation, and send output data obtained by the decryption,

 wherein the transmitting apparatus having:

10 a data analyzing portion to analyze information of the input data according to a predetermined instruction, and output analysis information;

 a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;

09856172.041804

15 a Field Programmable Gate Array (FPGA) circuit data generating portion to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a circuit configuration, and generate and output second circuit data;

20 a selector to select the plurality of circuit data according to an instruction of the selection signal, and output the first circuit data for encryption to the FPGA circuit data generating portion depending upon the selected circuit data;

25 a variable configuration processing circuit to update an own internal circuit depending upon the second circuit data output from the FPGA circuit data generating portion, output a completion posting signal when the update of the internal circuit is completed, and send to the network encrypted data obtained by encryption of held input data; and

30 an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input data the input data which has been held therein to the variable configuration processing circuit, and

the receiving apparatus having:

35 a data analyzing portion to analyze according to a predetermined instruction information of the encrypted data input from the network, and output analysis data;

40 a plurality of FPGA circuit data generating portions to output a selection signal depending upon the analysis data from the data analyzing portion, take as input first circuit data for update of a circuit configuration, and generate and output second circuit data;

a plurality of data circuit portions to hold circuit data used for specification of a cryptographic algorithm;

a selector to select the plurality of circuit data according to an

4001279860

instruction in the selection signal, and output to the FPGA circuit data generating portion the first circuit data used for decryption depending upon the selected circuit data;

a variable configuration processing circuit to update an own internal circuit for decryption depending upon the second circuit data output from the FPGA circuit data generating portion, output a completion posting signal when the update of the internal circuit is completed, and send decrypted output data obtained by decryption of encrypted data of held input data;

an encryption/decryption data holding portion to receive the completion posting signal, and additionally output as the held input data the input data which has been held therein to the variable configuration processing circuit;

the transmitting apparatus further comprising:

an encryption/decryption data holding portion to take as input and hold the input data, and take as input a circuit update posting signal to output as held data the input data which has been held therein;

a timer to generate and output a selector control signal at regular intervals;

a plurality of ROMs in which circuit data used for specification of a cryptographic algorithm is stored;

a selector to select the plurality of ROMs depending upon the selector control signal to take circuit data for encryption, and output circuit data used for specification of a cryptographic algorithm; and

a variable configuration processing circuit to receive the circuit data to output the circuit update posting signal, stop output of the held data, update an own internal circuit configuration depending upon the circuit data, stop the circuit update posting signal when the update is completed so as to resume output of the held data from the

4037403 3273860

75 encryption/decryption data holding portion, and take as input the held
data to perform an encryption operation through an updated internal
circuit configuration so as to send encrypted output data, and
the receiving apparatus having:

an encryption/decryption data holding portion to take as input
and hold the encrypted output data, and take as input a circuit update
80 posting signal so as to output as held data the input data which has
been held therein;

a timer to generate and output a selector control signal at
regular intervals;

85 a plurality of ROMs in which circuit data used for specification of
a cryptographic algorithm is stored;

a selector to select the plurality of ROMs depending upon the
selector control signal to take circuit data for encryption, and output
circuit data used for specification of a cryptographic algorithm; and

90 a variable configuration processing circuit to output the circuit
update posting signal in response to the circuit data so as to stop
output of the held data, update an own internal circuit configuration
depending upon the circuit data, stop the circuit update posting signal
when the update is completed so as to resume output of the held data
from the encryption/decryption data holding portion, and take as input
95 the held data to perform a decryption operation through an updated
internal circuit configuration so as to send decrypted output data.

38. An encryption-decryption apparatus according to claim 37,
wherein the variable configuration processing circuit is a Field
Programmable Gate Array.

FOST400+3/T95360